

Marathon sécurité d'un "move to cloud"

NBS System



NBS System

Expertise

Cloud – Web – Containers - Orchestrateurs

- Audit, Test d'Intrusion, Forensic
- DevSecOps
- Soc, SecOps
- Cyber-entraînement, Sensibilisation
- CerberHost



NBS System, Groupe Oceanet Technology, assure la sécurité informatique de plateformes web & SI depuis 1999 et accompagne ses clients dans leur stratégie Move to Cloud.

Regis Saint-Paul, Directeur

Guillaume Sevestre, RSSI

À l'opposé d'un simple projet de Lift-and-shift ...

Un **éditeur européen et global** de solution de **contact center** :

- Des centres de relation client jusqu'à plusieurs milliers de postes
- Sur un marché global
- Répondant aux normes les plus strictes (ISO27, PCI-DSS, HDS, cible SOC2 & CSA *)

Un projet **de transformation** ambitieux du modèles SaaS :

- Proximité & agilité à l'international via le **cloud public**
- Transformation applicative : **conteneurisation** et **one-release**

De nombreux acteurs à fédérer :

- Equipes internes (opération, dev, contrôle)
- Cloud provider (AWS pour débiter)
- Cloud Service Provider (CSP)
- Practice Sécurité (NBS System)

Intégrer la sécurité dès le cadrage du projet

Contraintes & Besoins

- Risques
- Besoins de conformité
- Exigences clients

Process

- Analyse des risques
- MAJ de la Politique de Sécurité des Plateformes

Règles & choix

- Modèle de Tenancy
- Cloisonnement Cloud <-> On-prem
- Guidelines sécu thématiques

Client Account
VPC

SaaS / CSP

Cloud (AWS)

Mise en œuvre des mesures & choix des outils

Une démarche itérative ...

Points d'adhérence et de rencontres avec la roadmap applicative et les autres projets internes (IAM - Fédération)

Existant **on-prem** et trajectoire **Mutlicloud** :

- Choix d'outils transverses adaptables aux 2 environnements (+ n)
- Focus sur la chaîne **d'intégration continue** (CI/CD) mutualisée

Services de **sécurité managés** du CP profitables, après étude du lock-in

Toute mesure doit prendre en compte **l'évolution des services managés**

... pilotée par les risques

Audit & Contrôle

Matrice de **couverture des exigences de sécurité** vérifiée



Utilisation d'outils de **contrôle de conformité** disponibles (Cloud Provider, éditeurs tiers)

Direction de l'entreprise et practice sécurité alignés sur la nécessité **d'un audit préalable** :

- Pentest en cours \ **applicatif, container** et **cloisonnement**



Une affaire de compromis

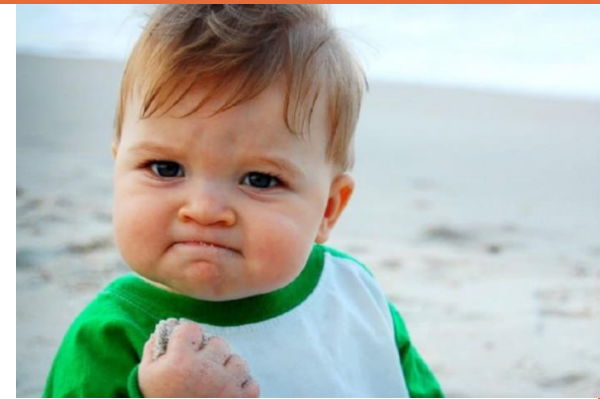
Les solutions disponibles contraignent les choix

Exemple:

- Chiffrement : très accessible et facilement systématisable
- Mais... *Bring Your Own Key (*)* : très contraignant
- Filtrage et segmentation applicative

() Utilisation de vos propres clés de chiffrement*

Il n'y a pas de petites victoires en SSI ...



Gouvernance :

- Politique de sécurité **opérationnelle** « cloud/container ready », en évolution
- Approche **risque et conformité** sur une démarche incrémentale

Technique :



- Isolation des clients via tenants/comptes aws dédiés
- Isolation des environnements : dev , ... , preprod, prod , ainsi que cloud / onprem
- **Politiques de sécurité globales** appliquées aux tenant/comptes (SCP), as code
- Gestion des droits sur les utilisateurs aws **par rôles + MFA** (prêt pour la fédération)
- Automatisation de points de contrôle/audit de la sécurité (aws config, scan images)
- Gestion des **maj et des vulnérabilités** (hotes et container)
- Sécurité runtime host et containers (comportemental + AV sur les hôtes)

Conclusion & next steps

Influence mutuelle des stratégies d'évolution de l'application, des clouds et de la sécurité...

... mais les principes de sécurité restent immuables (séparation des rôles, cloisonnement, contrôles, surface d'exposition)

Beaucoup reste à faire, mais une méthodologie sécurité qui fonctionne et permet la convergence des besoins métiers et sécurité sans conflit

Comment?

- Lien fort entre gouvernance et opérations
- À chaque itération : **engagement** de toutes **les parties** y compris **la direction** sur les risques et la roadmap

Venez échanger sur ces sujets ...



Stand 55 – Niveau Diaghilev

www.nbs-system.com